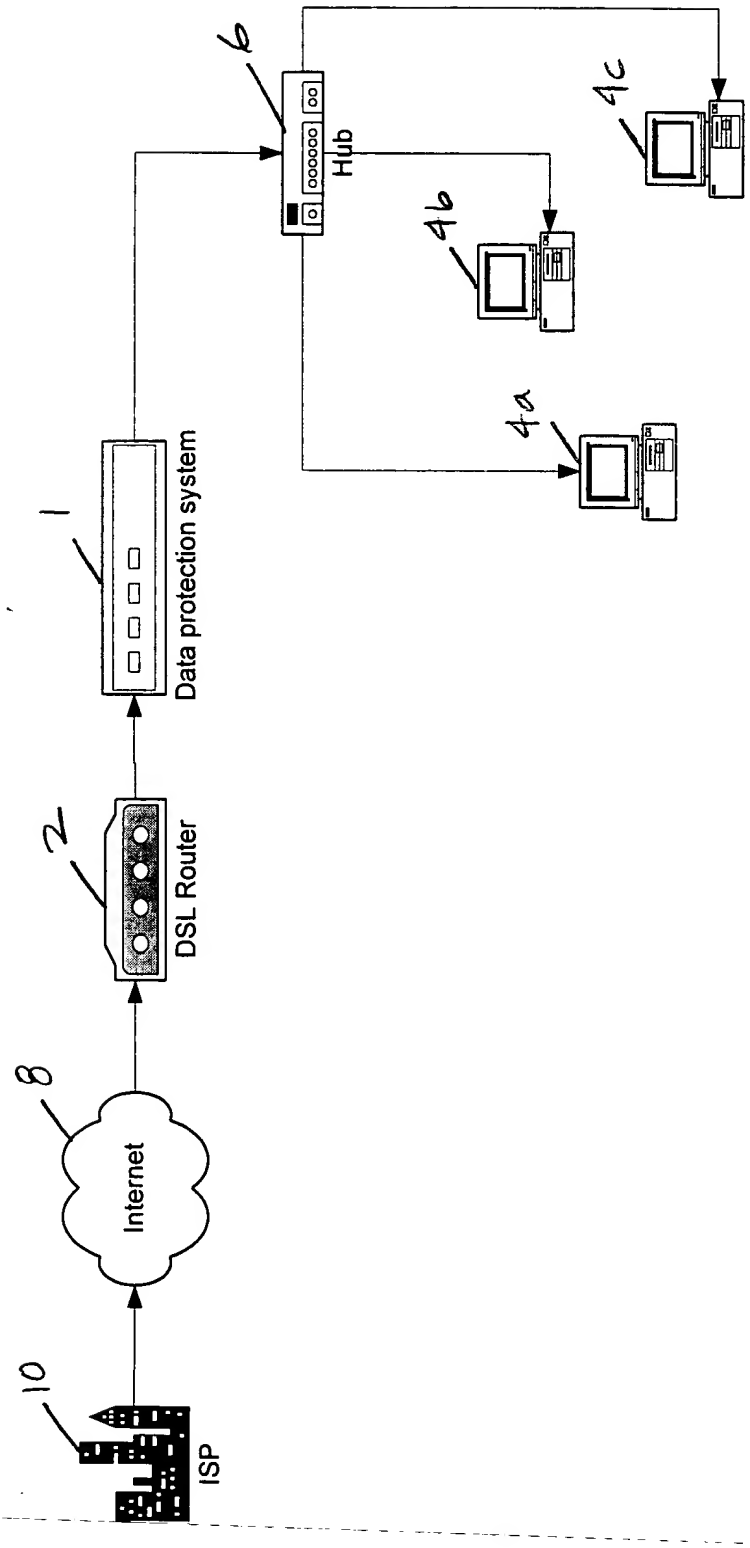
ISP
10
Internet
8
DSL Router
2
Data protection system
1
Hub
6
4a
4b
4c

FIG. 1A

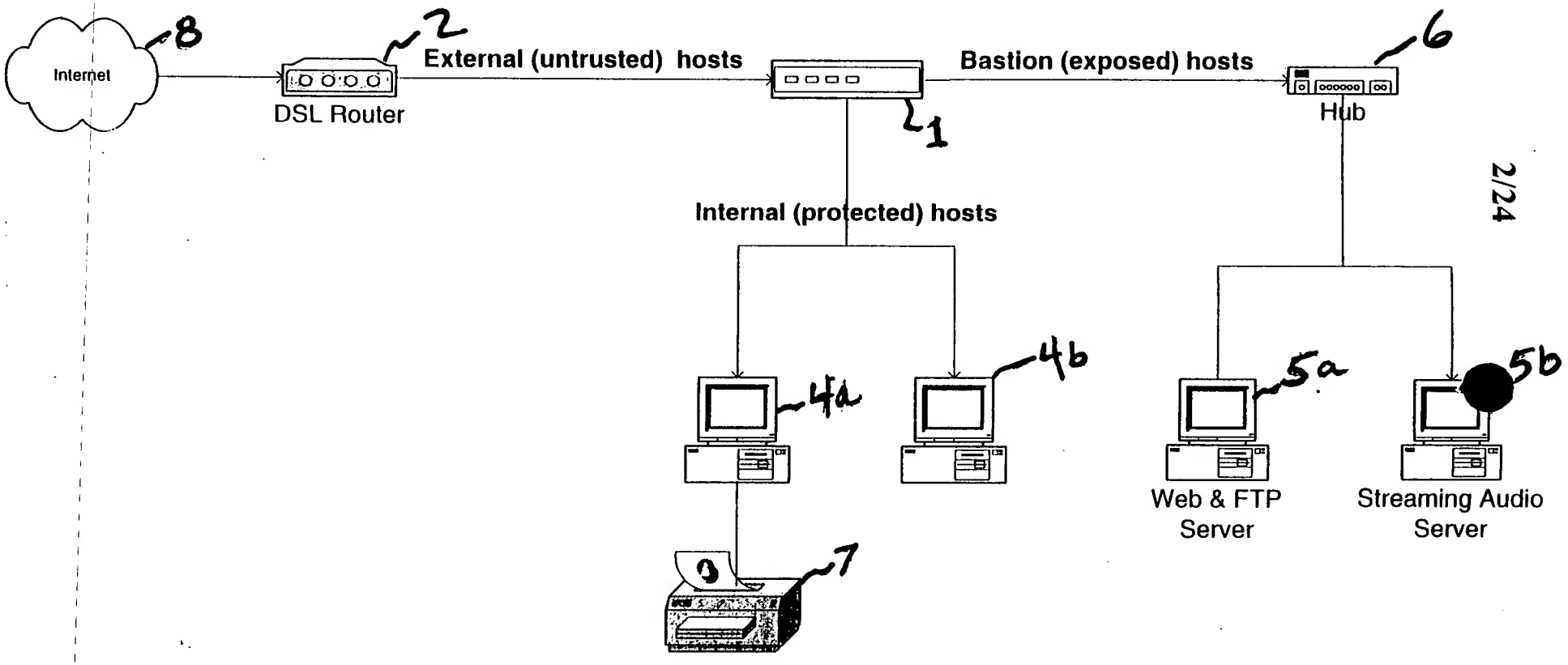
Internet
8
DSL Router
2
External (untrusted) hosts
1
Bastion (exposed) hosts
6
Hub
Internal (protected) hosts
4a
4b
5a
5b
Web & FTP Server
Streaming Audio Server
7

FIG. 1B

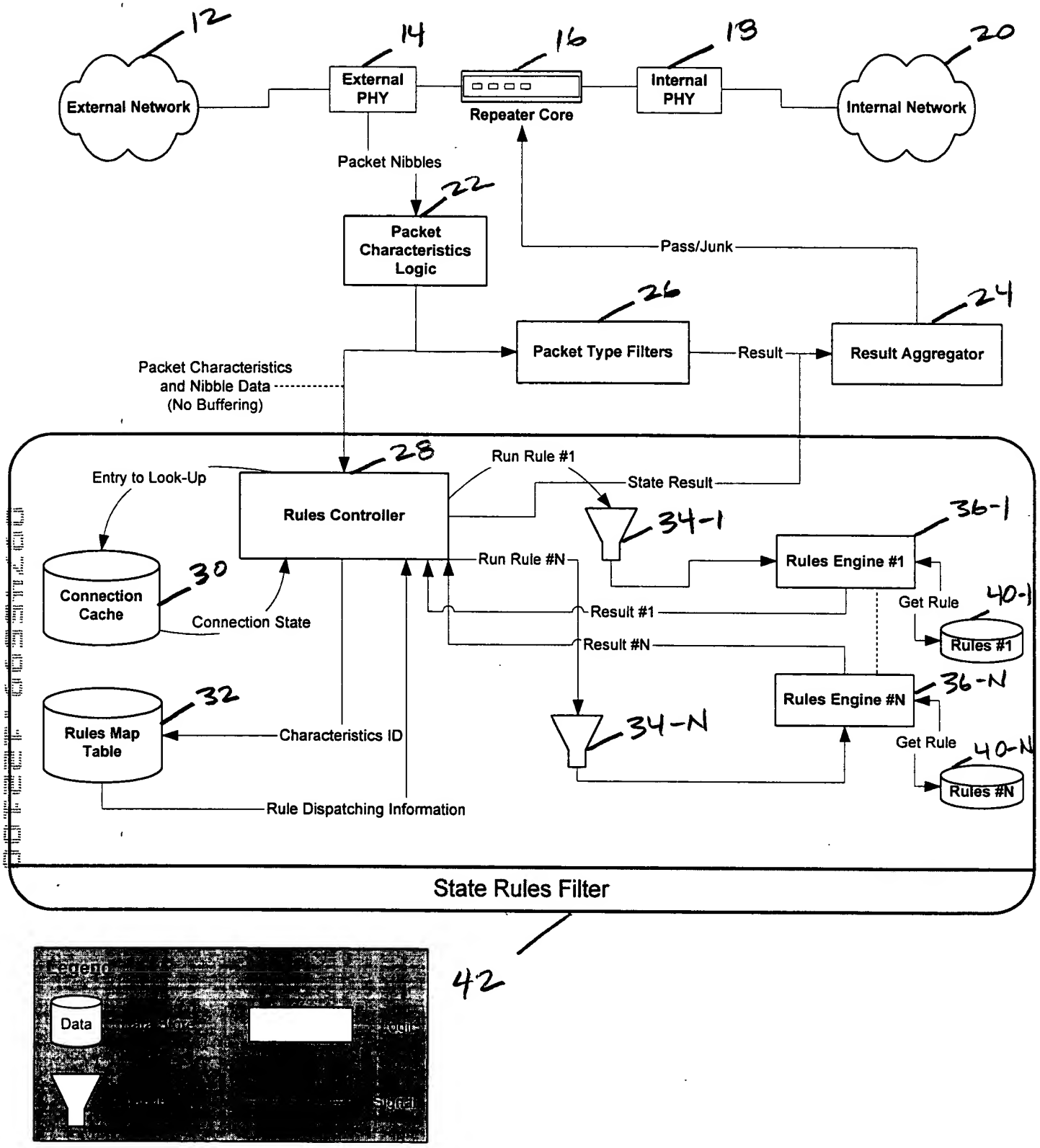
12
External Network
14
External PHY
16
Repeater Core
18
Internal PHY
20
Internal Network
Packet Nibbles
22
Packet Characteristics Logic
Pass/Junk
26
Packet Type Filters
Result
24
Result Aggregator
Packet Characteristics and Nibble Data (No Buffering)
28
Rules Controller
Entry to Look-Up
Run Rule #1
State Result
34-1
36-1
Rules Engine #1
Run Rule #N
30
Connection Cache
Connection State
Result #1
Get Rule
40-1
Rules #1
Result #N
Rules Engine #N
36-N
32
Rules Map Table
Characteristics ID
34-N
Get Rule
40-N
Rules #N
Rule Dispatching Information
State Rules Filter
42
Legend
Data

FIG. 2

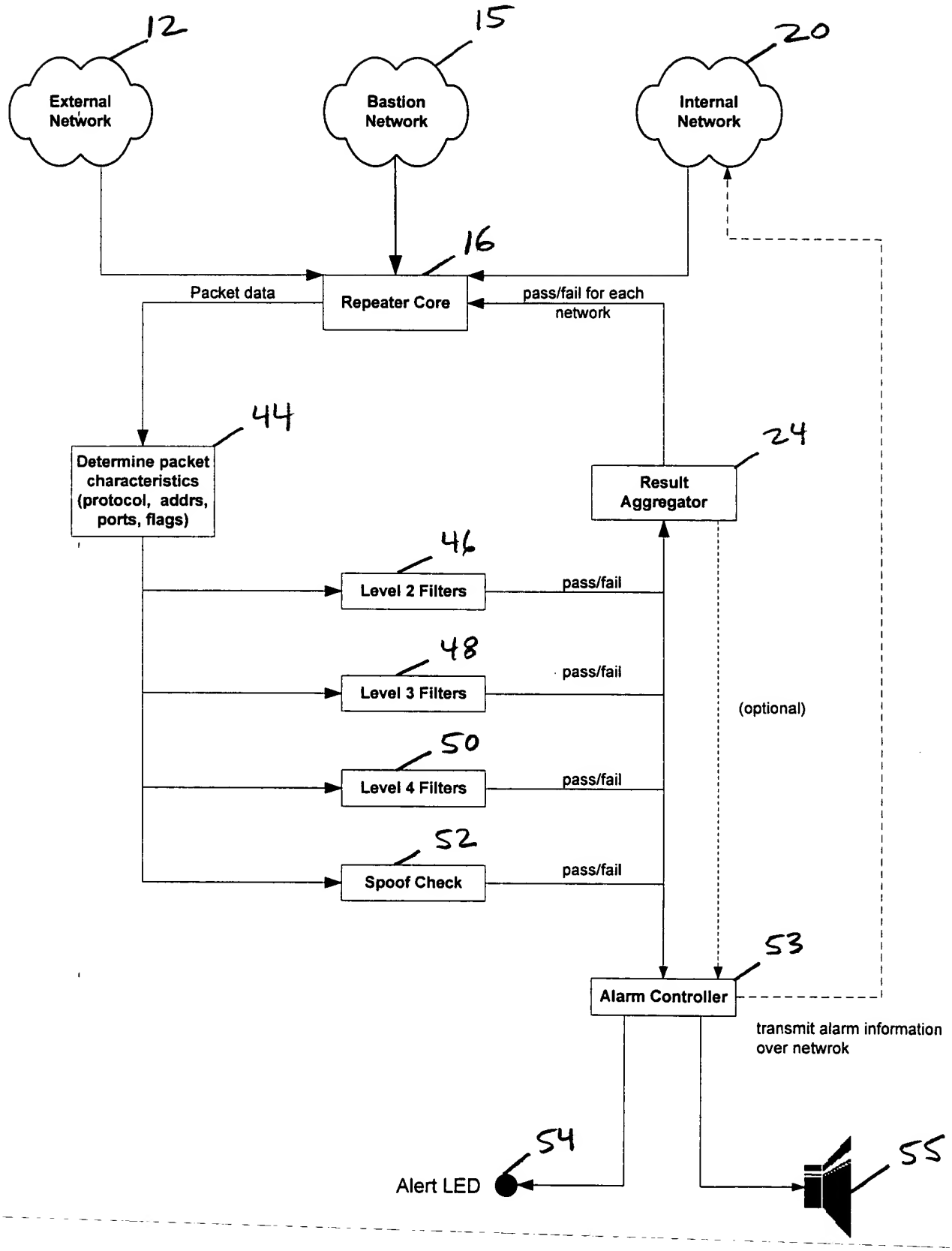
12
External Network
15
Bastion Network
20
Internal Network
16
Repeater Core
Packet data
pass/fail for each network
44
Determine packet characteristics (protocol, addrs, ports, flags)
24
Result Aggregator
46
Level 2 Filters
pass/fail
48
Level 3 Filters
pass/fail
(optional)
50
Level 4 Filters
pass/fail
52
Spoof Check
pass/fail
53
Alarm Controller
transmit alarm information over netwrok
54
Alert LED
55

FIG. 3

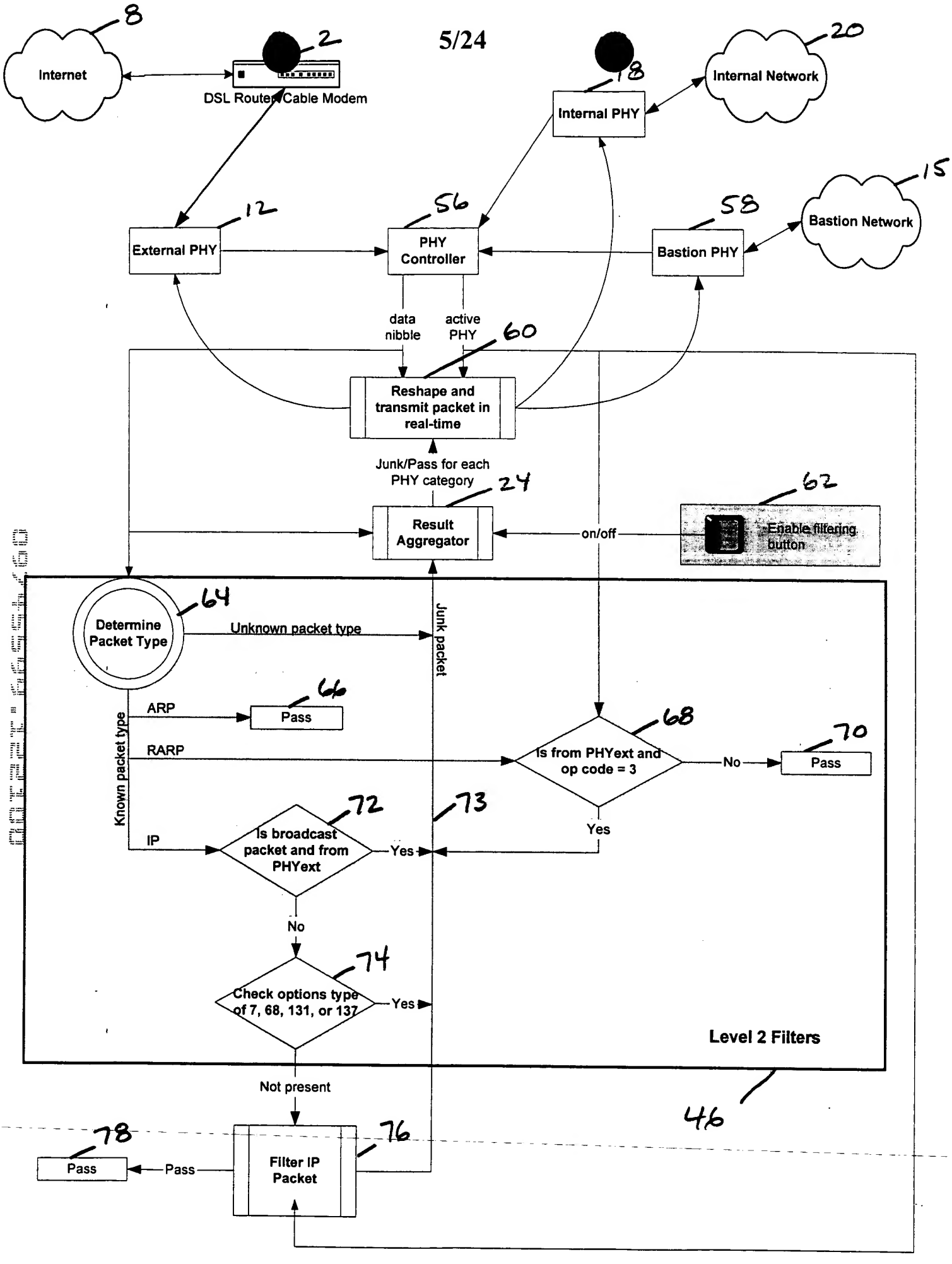
8
Internet
2
DSL Router/Cable Modem
18
Internal PHY
20
Internal Network
15
Bastion Network
12
External PHY
56
PHY Controller
58
Bastion PHY
data nibble
active PHY
60
Reshape and transmit packet in real-time
Junk/Pass for each PHY category
24
Result Aggregator
on/off
62
Enable filtering button
64
Determine Packet Type
Unknown packet type
Junk packet
ARP
66
Pass
Known packet type
RARP
68
Is from PHYext and op code = 3
No
70
Pass
Yes
IP
72
Is broadcast packet and from PHYext
73
Yes
No
74
Check options type of 7, 68, 131, or 137
Yes
Level 2 Filters
46
Not present
78
Pass
Pass
Filter IP Packet
76

FIG. 4

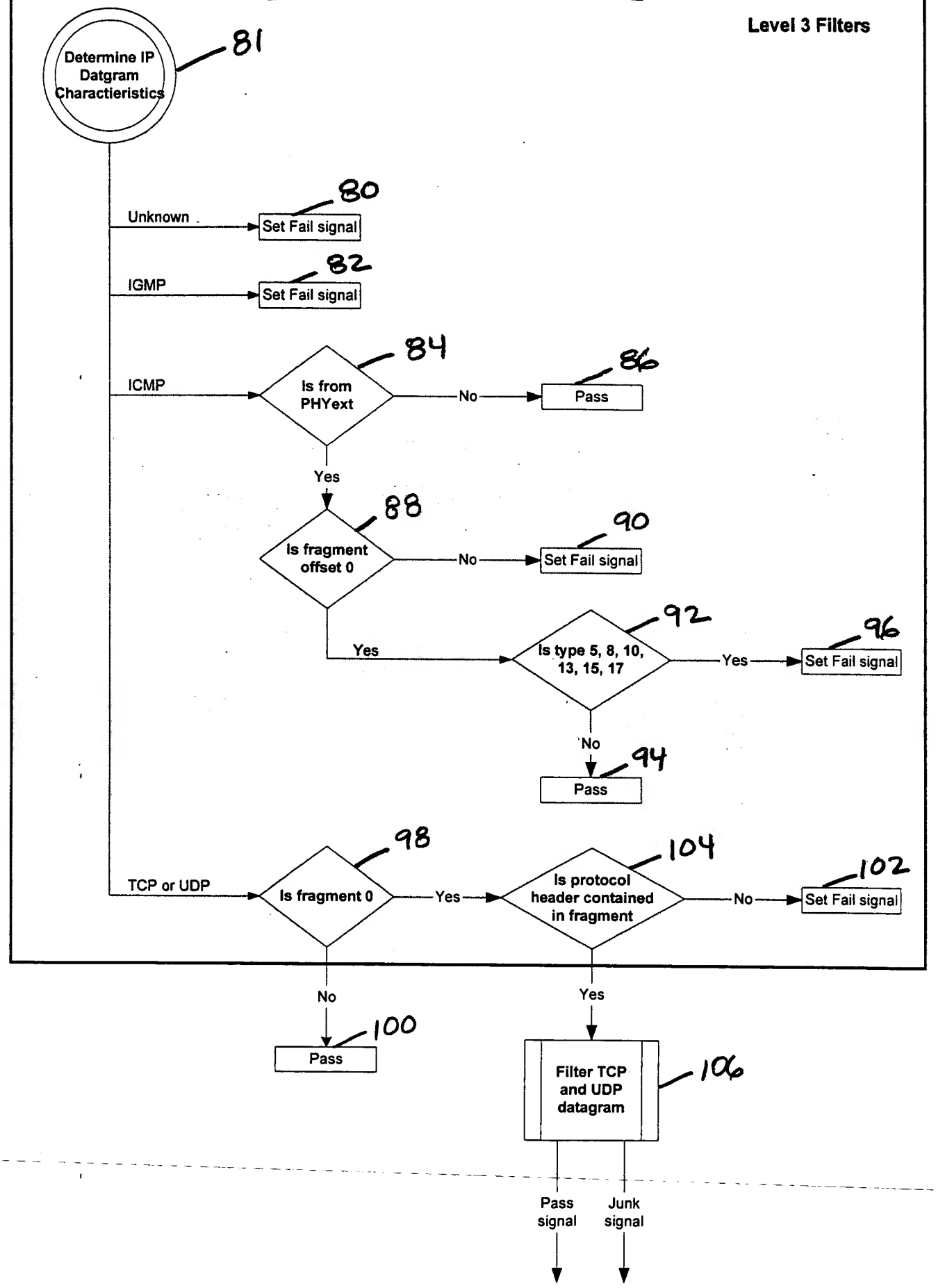
Level 3 Filters
Determine IP Datgram Charactieristics
81
Unknown
80
Set Fail signal
IGMP
82
Set Fail signal
ICMP
Is from PHYext
84
No
Pass
86
Yes
Is fragment offset 0
88
No
Set Fail signal
90
Yes
Is type 5, 8, 10, 13, 15, 17
92
Yes
Set Fail signal
96
No
Pass
94
TCP or UDP
Is fragment 0
98
Yes
Is protocol header contained in fragment
104
No
Set Fail signal
102
No
Pass
100
Yes
Filter TCP and UDP datagram
106
Pass signal
Junk signal

FIG. 5

TCP and UDP packets are evaluated for pass or fail in parallel (other protocols also handled simultaneously)

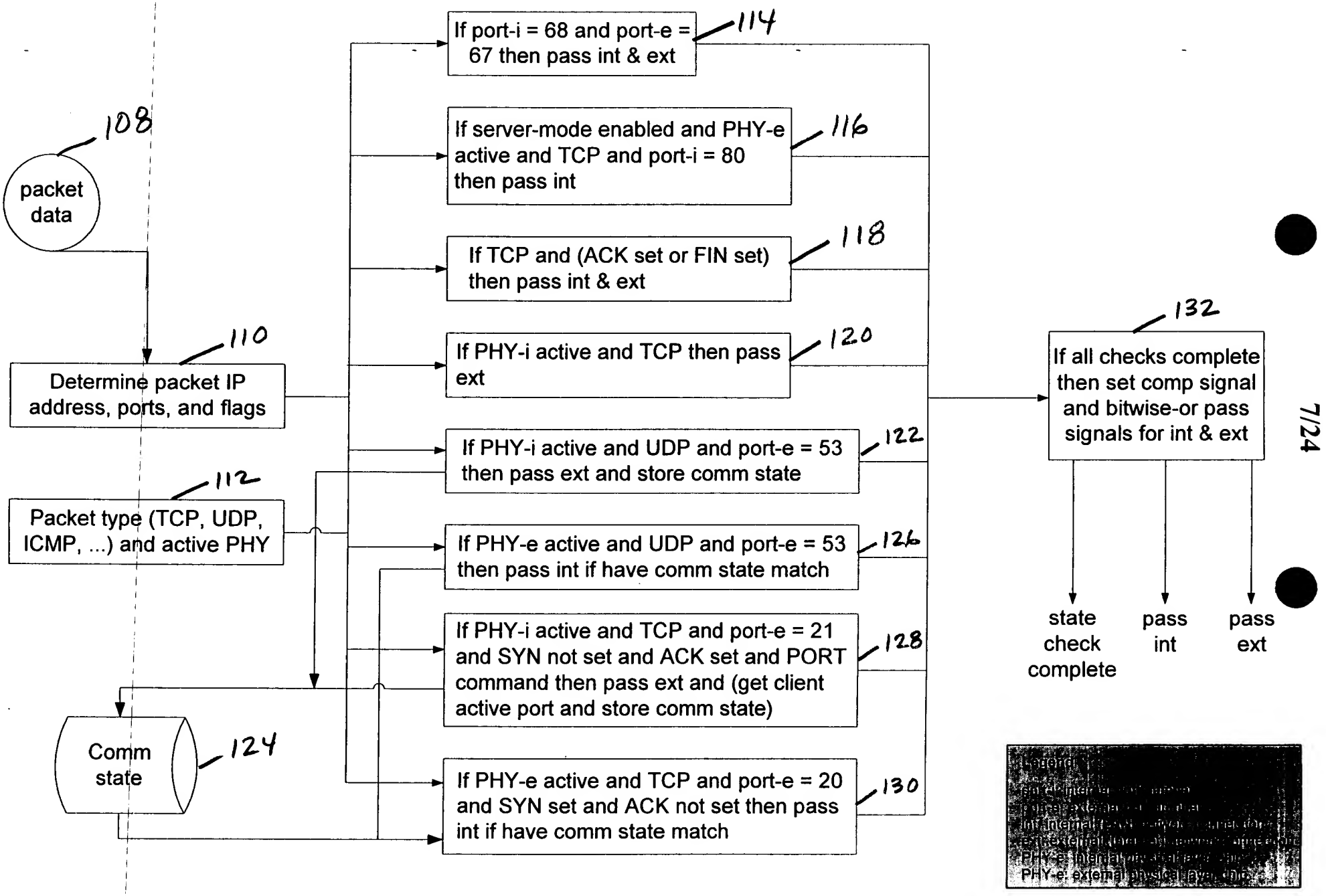


FIG. 6

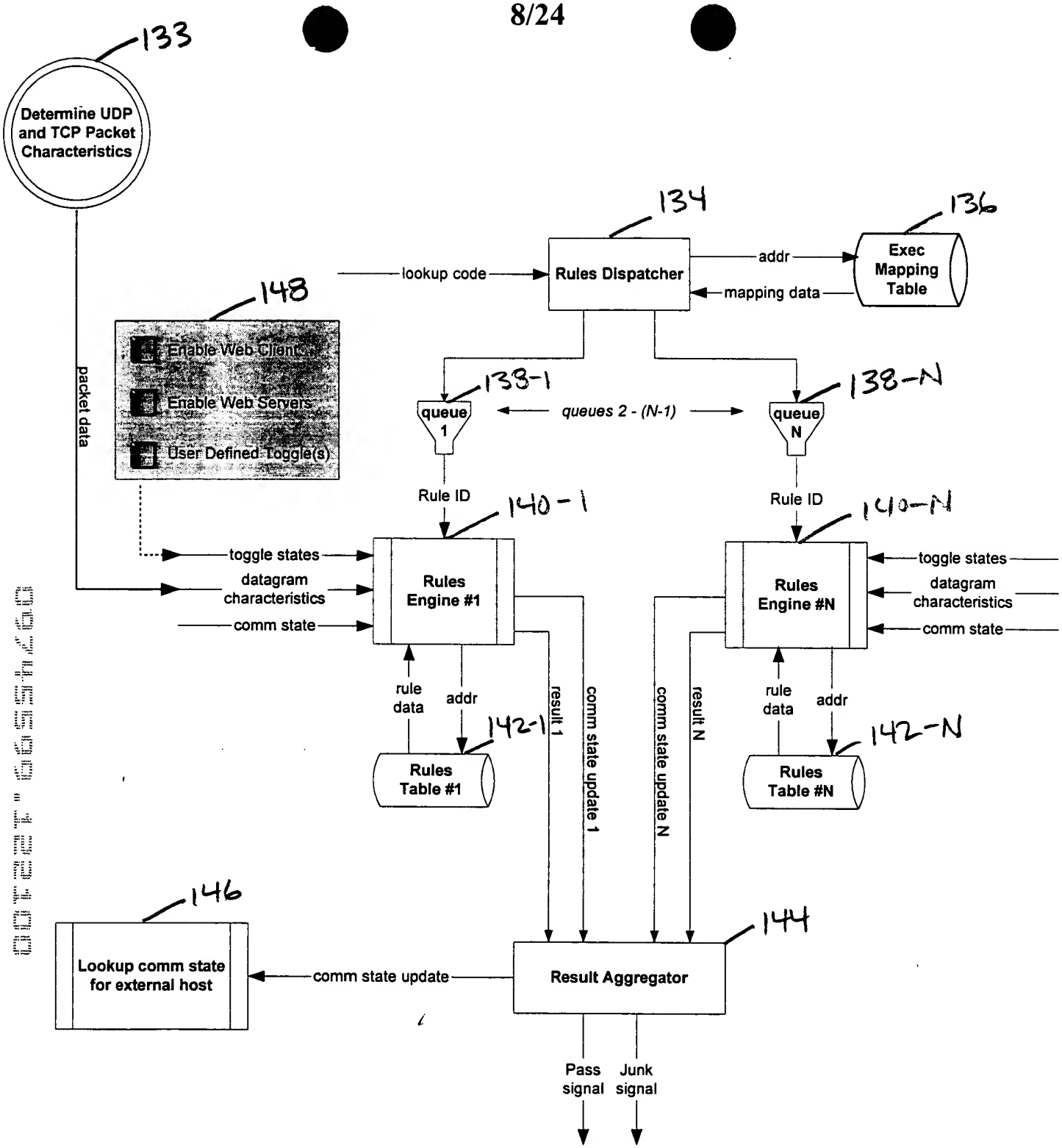
133
Determine UDP and TCP Packet Characteristics
134
Rules Dispatcher
lookup code
addr
mapping data
136
Exec Mapping Table
148
Enable Web Client
Enable Web Servers
User Defined Toggle(s)
packet data
138-1
queue 1
queues 2 - (N-1)
queue N
138-N
Rule ID
Rule ID
140-1
140-N
toggle states
datagram characteristics
comm state
Rules Engine #1
Rules Engine #N
rule data
addr
result 1
comm state update 1
comm state update N
result N
142-1
142-N
Rules Table #1
Rules Table #N
146
Lookup comm state for external host
comm state update
144
Result Aggregator
Pass signal
Junk signal

FIG. 7

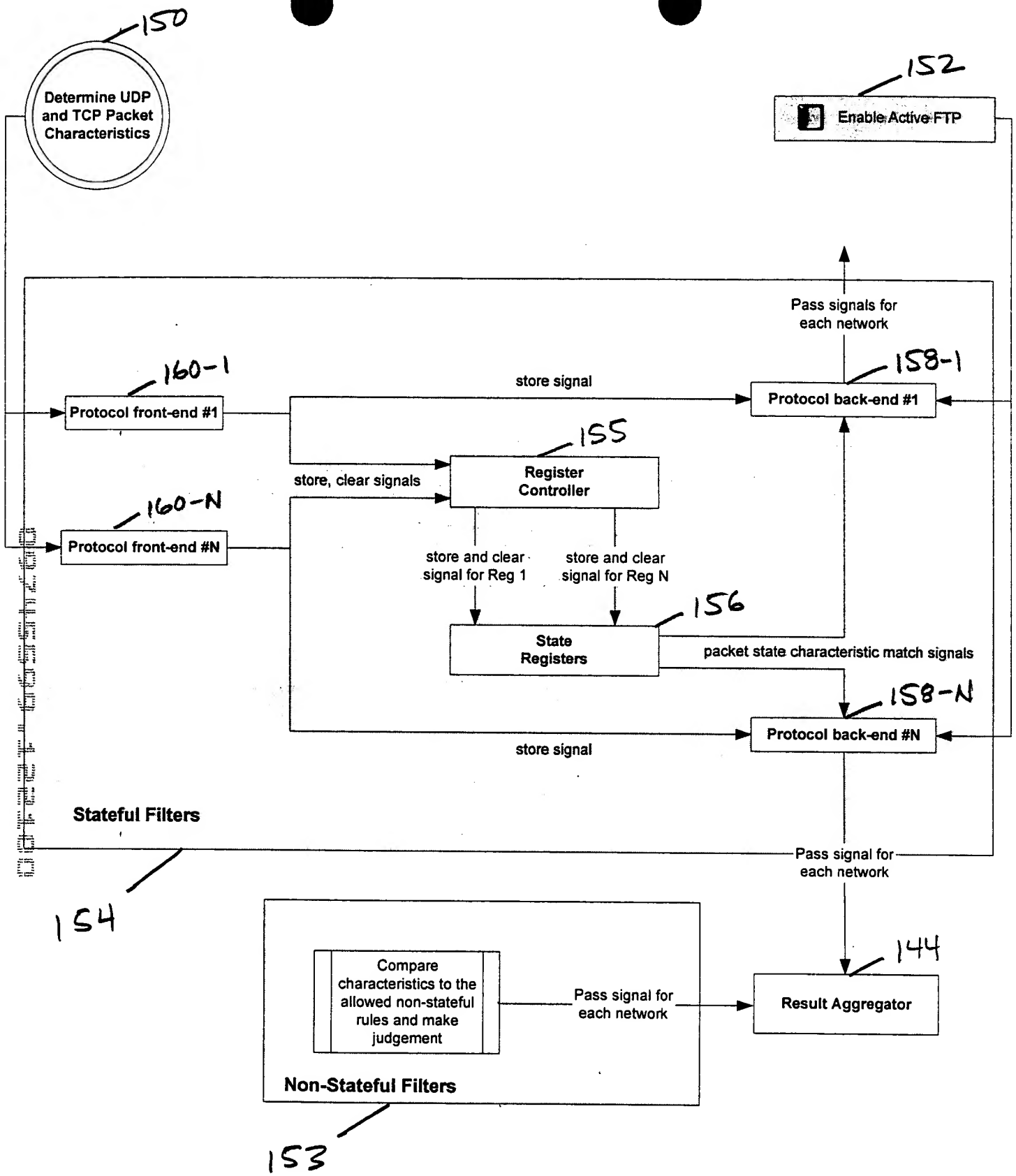
150
Determine UDP and TCP Packet Characteristics
152
Enable Active FTP
Pass signals for each network
160-1
Protocol front-end #1
store signal
158-1
Protocol back-end #1
155
Register Controller
store, clear signals
160-N
Protocol front-end #N
store and clear signal for Reg 1
store and clear signal for Reg N
156
State Registers
packet state characteristic match signals
158-N
Protocol back-end #N
store signal
Stateful Filters
154
Pass signal for each network
144
Result Aggregator
Compare characteristics to the allowed non-stateful rules and make judgement
Pass signal for each network
Non-Stateful Filters
153

FIG. 8

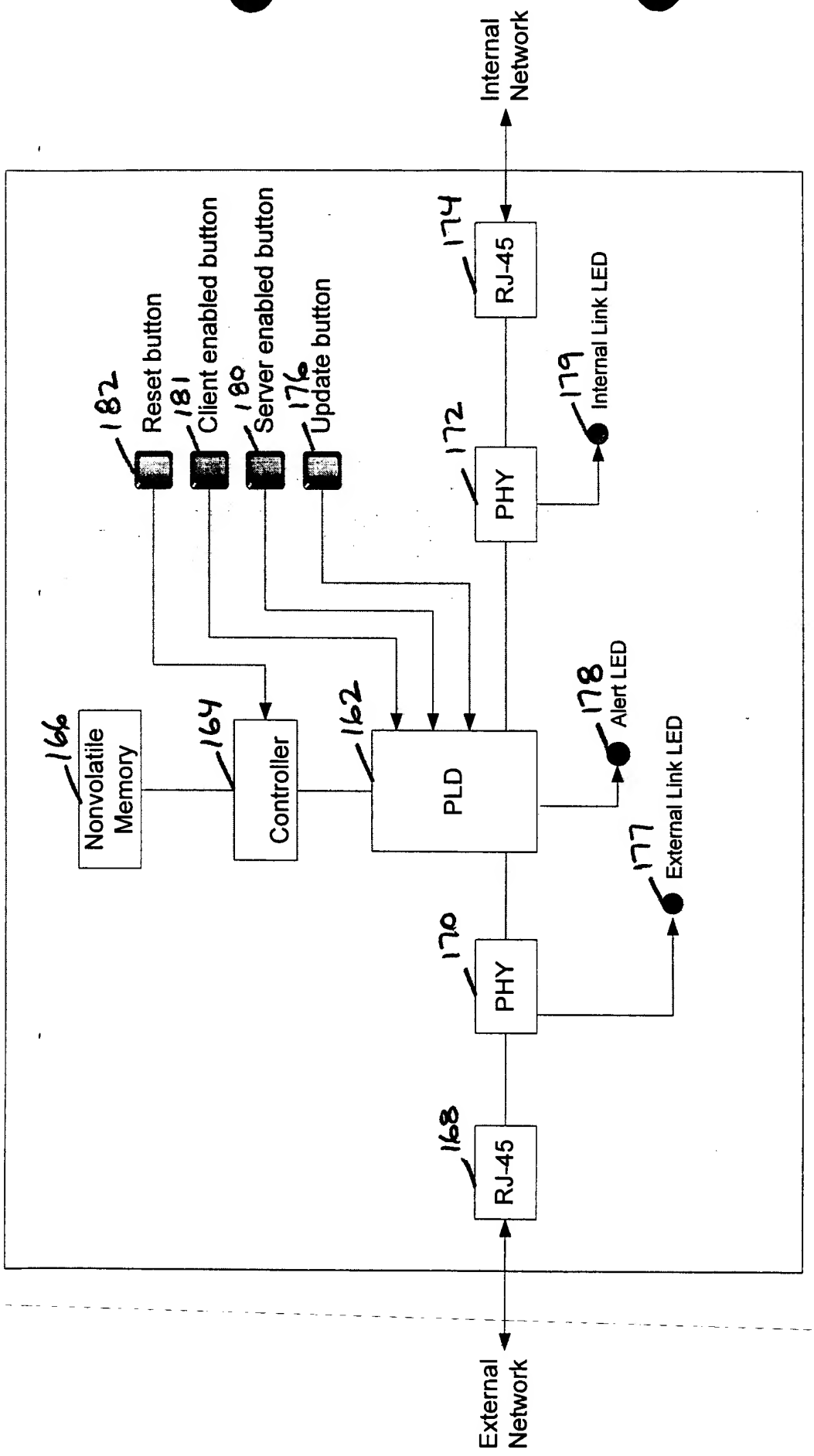
Internal Network
External Network
RJ-45
168
PHY
170
PHY
172
RJ-45
174
PLD
162
Controller
164
Nonvolatile Memory
166
Reset button
182
Client enabled button
181
Server enabled button
180
Update button
176
Alert LED
178
External Link LED
177
Internal Link LED
179

FIG. 9

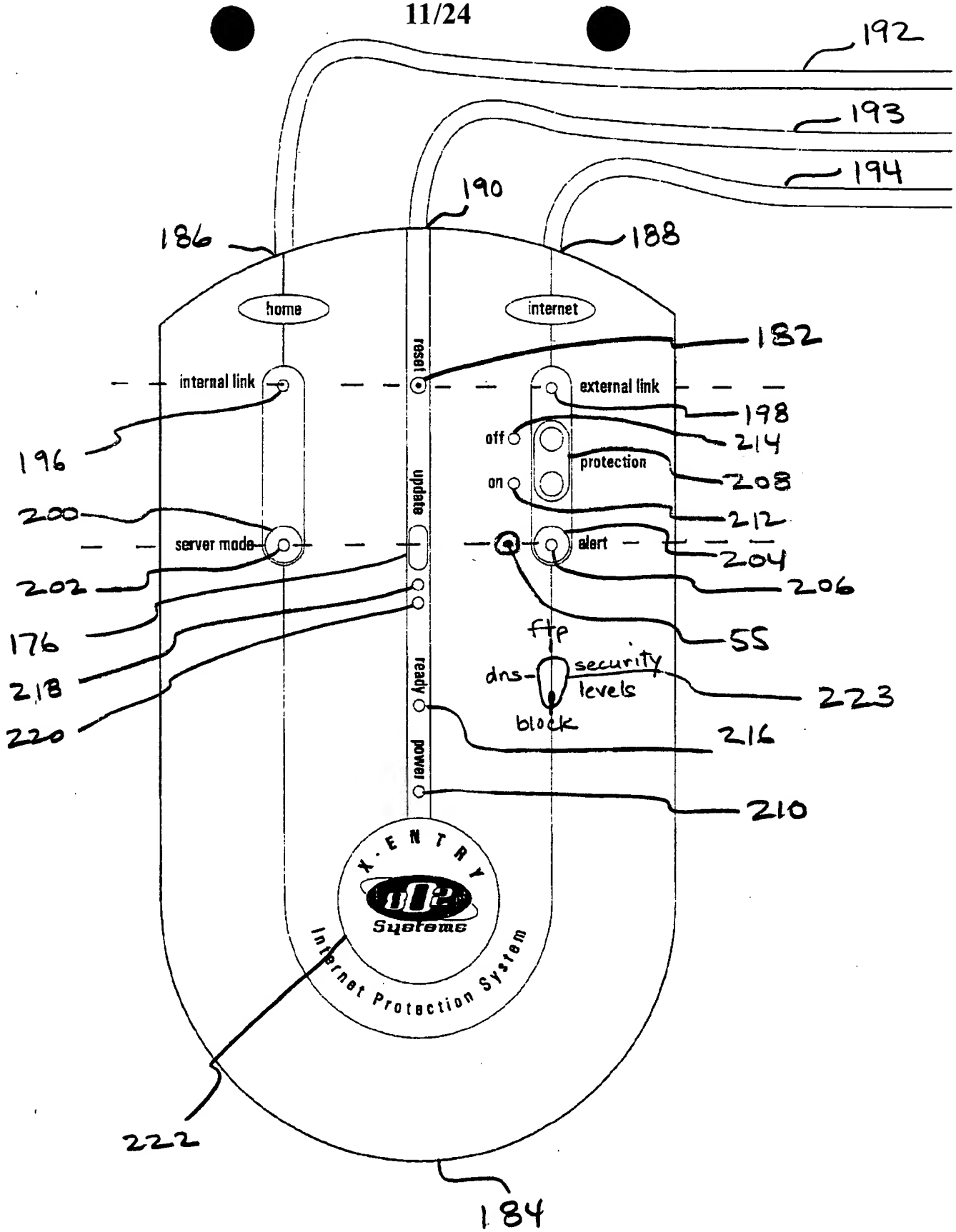
192
193
194
190
186
188
home
internet
reset
182
internal link
external link
198
196
off
214
protection
208
on
212
200
update
server mode
alert
204
202
206
176
55
ftp
dns-
security
levels
223
218
block
220
ready
216
power
210
X-ENTRY
Systems
Internet Protection System
222
184

FIG. 10

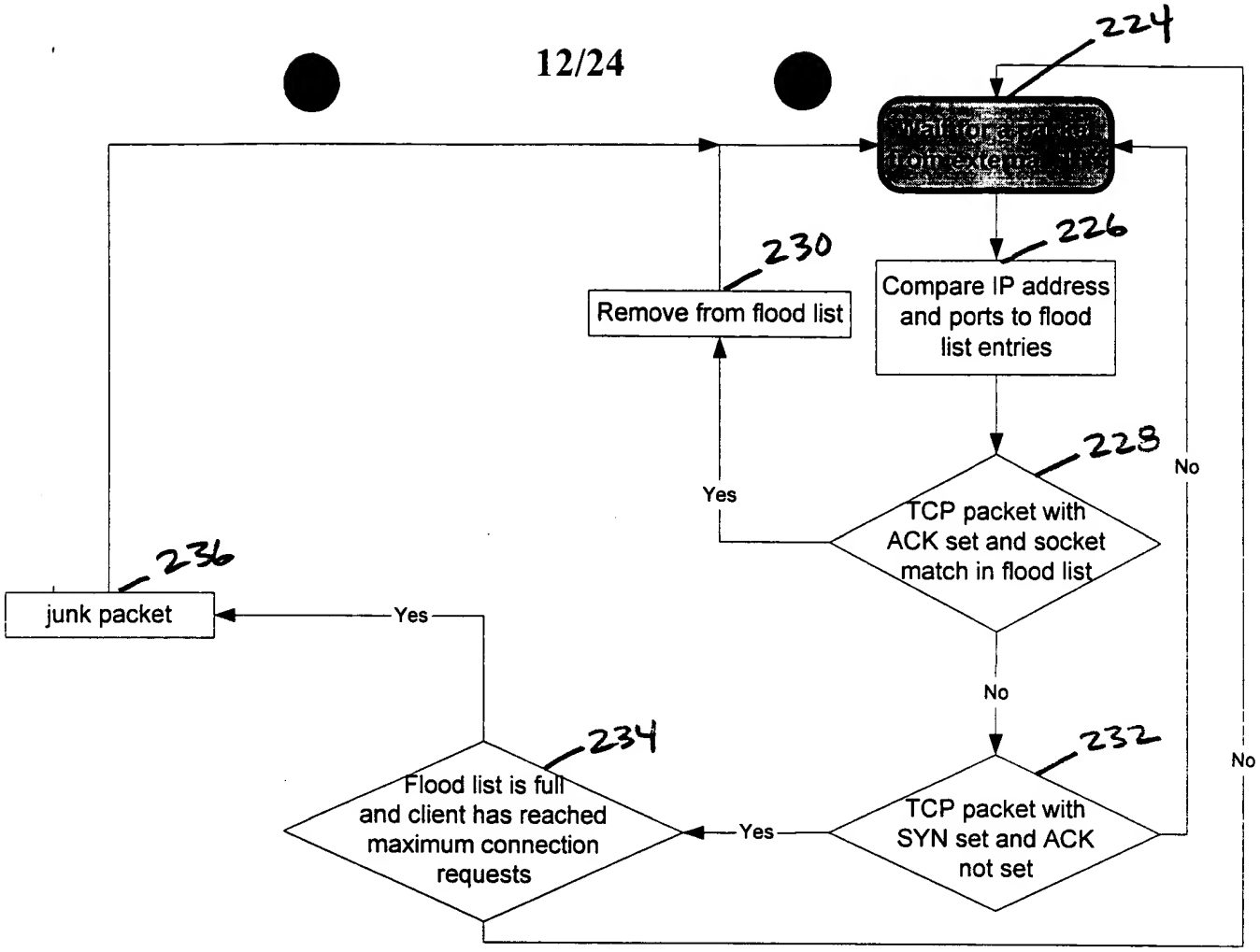
224
Wait for a packet from external PHY
226
Compare IP address and ports to flood list entries
228
TCP packet with ACK set and socket match in flood list
Yes
No
230
Remove from flood list
232
TCP packet with SYN set and ACK not set
Yes
No
234
Flood list is full and client has reached maximum connection requests
Yes
236
junk packet

FIG. 11

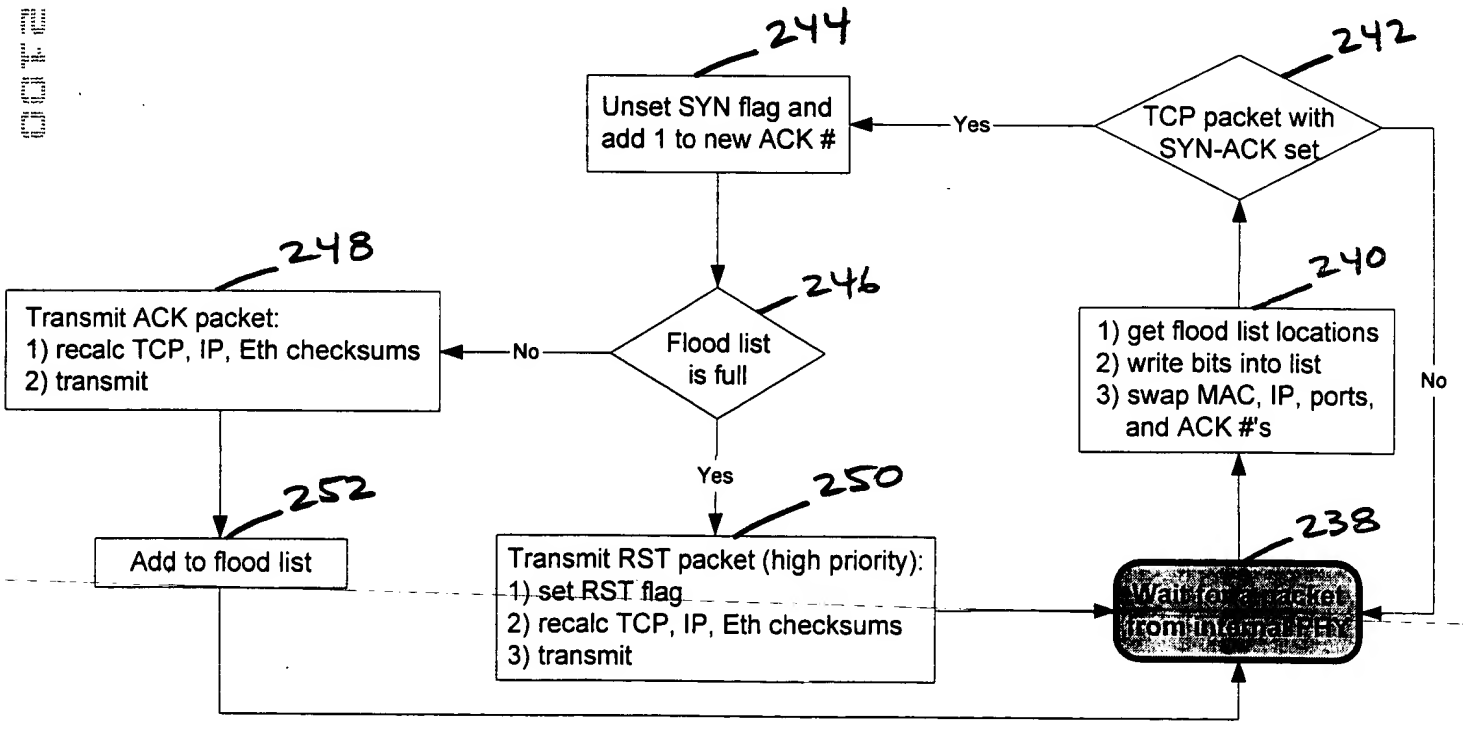
242
TCP packet with SYN-ACK set
Yes
244
Unset SYN flag and add 1 to new ACK #
240
1) get flood list locations
2) write bits into list
3) swap MAC, IP, ports, and ACK #'s
No
246
Flood list is full
No
248
Transmit ACK packet:
1) recalc TCP, IP, Eth checksums
2) transmit
Yes
250
Transmit RST packet (high priority):
1) set RST flag
2) recalc TCP, IP, Eth checksums
3) transmit
252
Add to flood list
238
Wait for a packet from internal PHY

FIG. 12

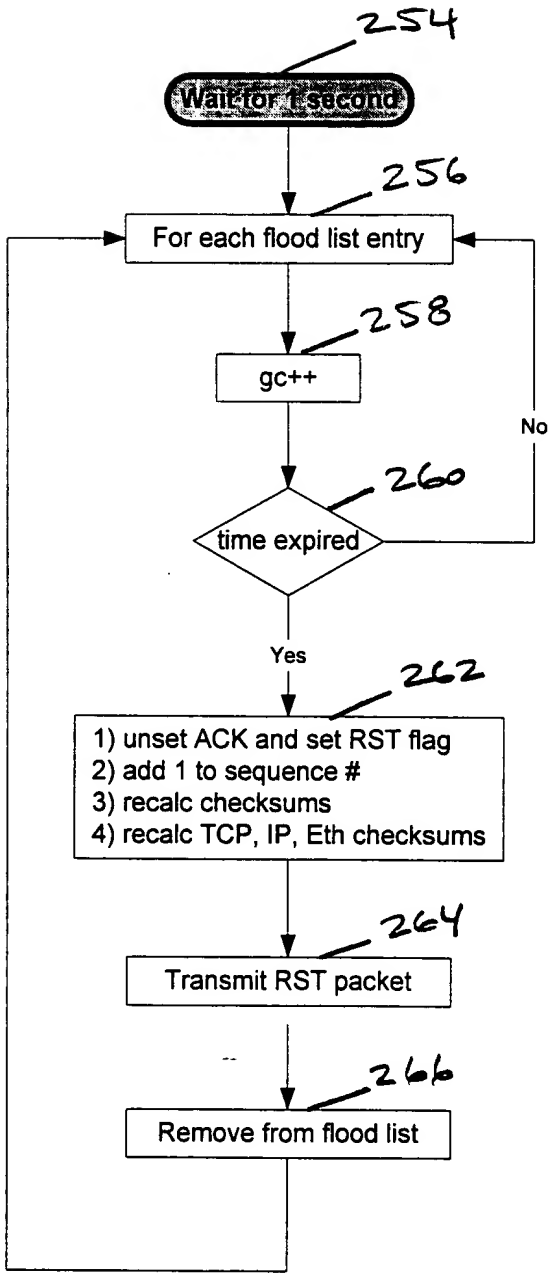
254
Wait for 1 second
256
For each flood list entry
258
gc++
No
260
time expired
Yes
262
1) unset ACK and set RST flag
2) add 1 to sequence #
3) recalc checksums
4) recalc TCP, IP, Eth checksums
264
Transmit RST packet
266
Remove from flood list

FIG. 13

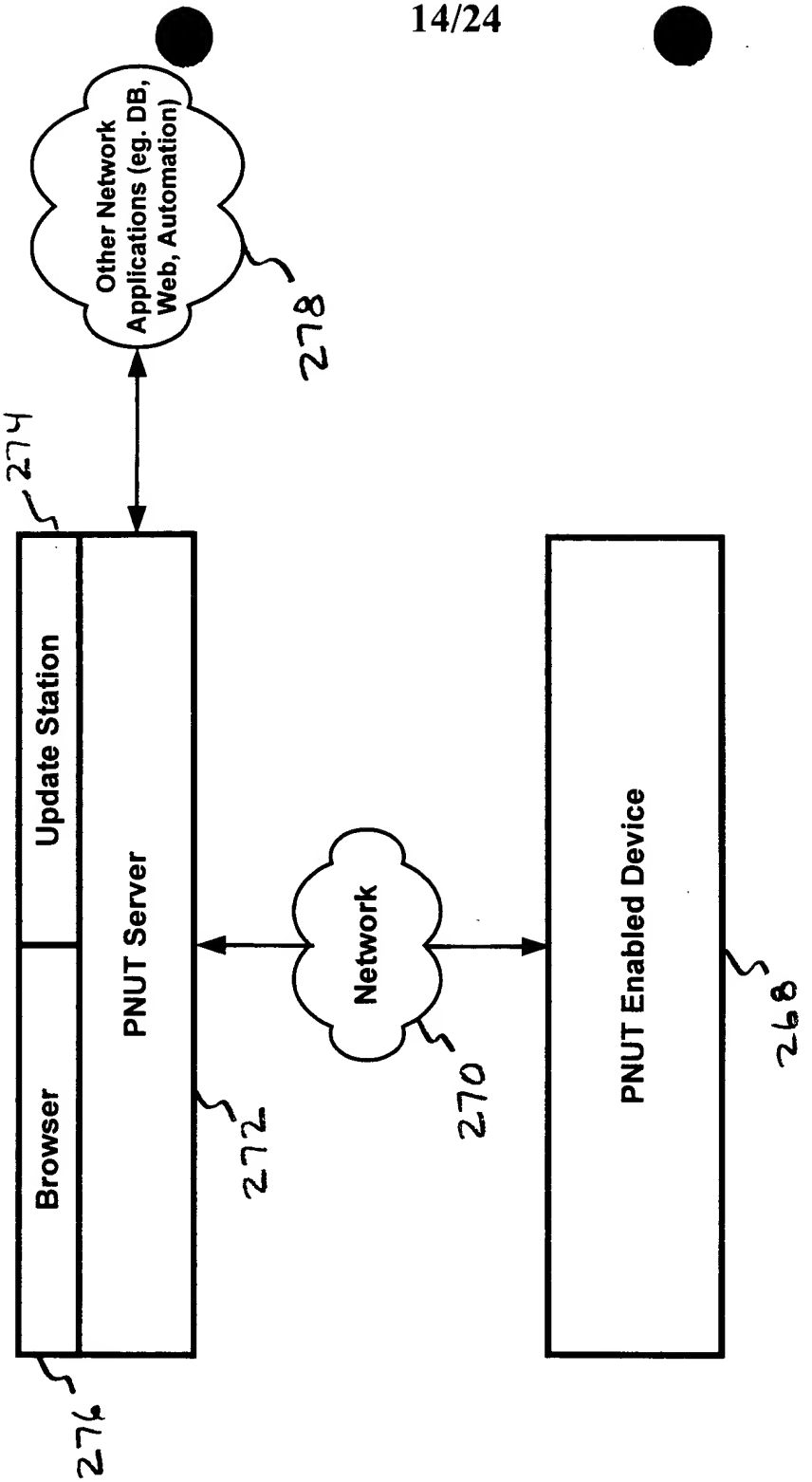
Other Network Applications (eg. DB, Web, Automation)
278
274
Update Station
PNUT Server
Browser
276
272
Network
270
PNUT Enabled Device
268

FIG. 14

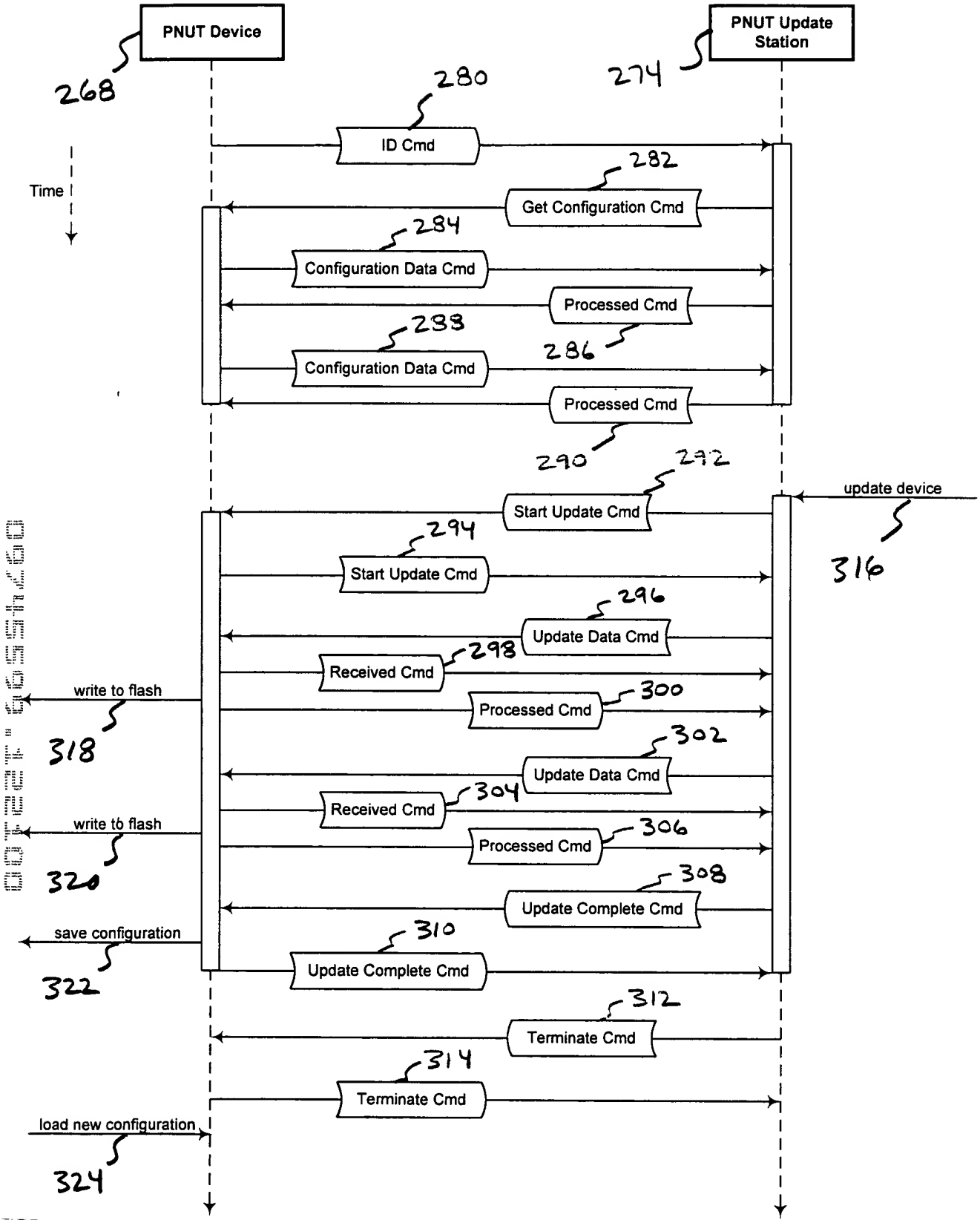
PNUT Device
268
PNUT Update Station
274
280
ID Cmd
Time
282
Get Configuration Cmd
284
Configuration Data Cmd
Processed Cmd
288
Configuration Data Cmd
286
Processed Cmd
290
292
Start Update Cmd
update device
316
294
Start Update Cmd
296
Update Data Cmd
298
Received Cmd
write to flash
318
Processed Cmd
300
302
Update Data Cmd
304
Received Cmd
write to flash
320
Processed Cmd
306
308
Update Complete Cmd
save configuration
322
310
Update Complete Cmd
312
Terminate Cmd
314
Terminate Cmd
load new configuration
324

FIG. 15

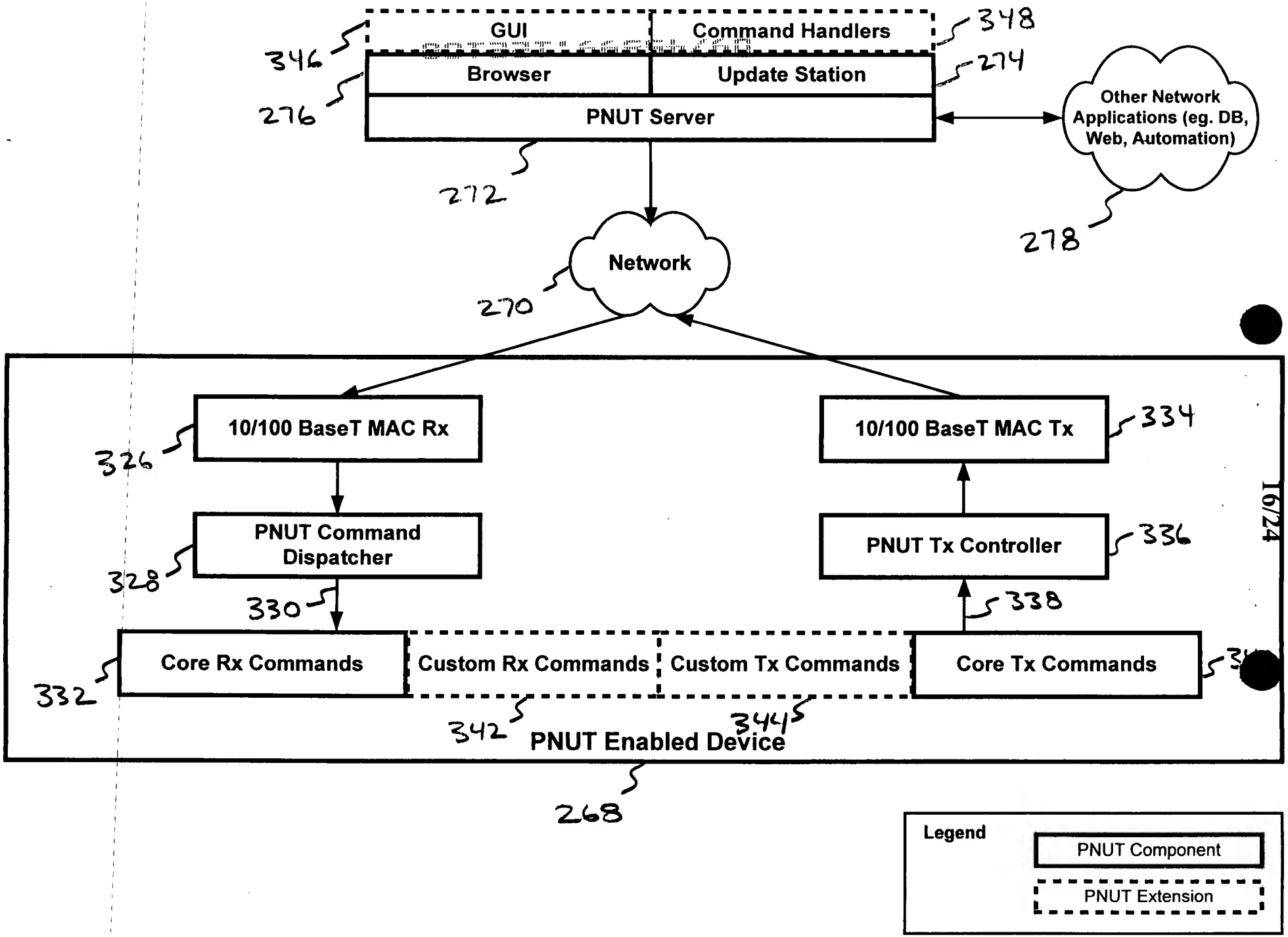
GUI
Command Handlers
348
346
Browser
Update Station
274
276
PNUT Server
272
Other Network Applications (eg. DB, Web, Automation)
278
Network
270
10/100 BaseT MAC Rx
326
10/100 BaseT MAC Tx
334
PNUT Command Dispatcher
328
PNUT Tx Controller
336
330
338
Core Rx Commands
Custom Rx Commands
Custom Tx Commands
Core Tx Commands
332
342
344
PNUT Enabled Device
268
16/24
Legend
PNUT Component
PNUT Extension

FIG. 16

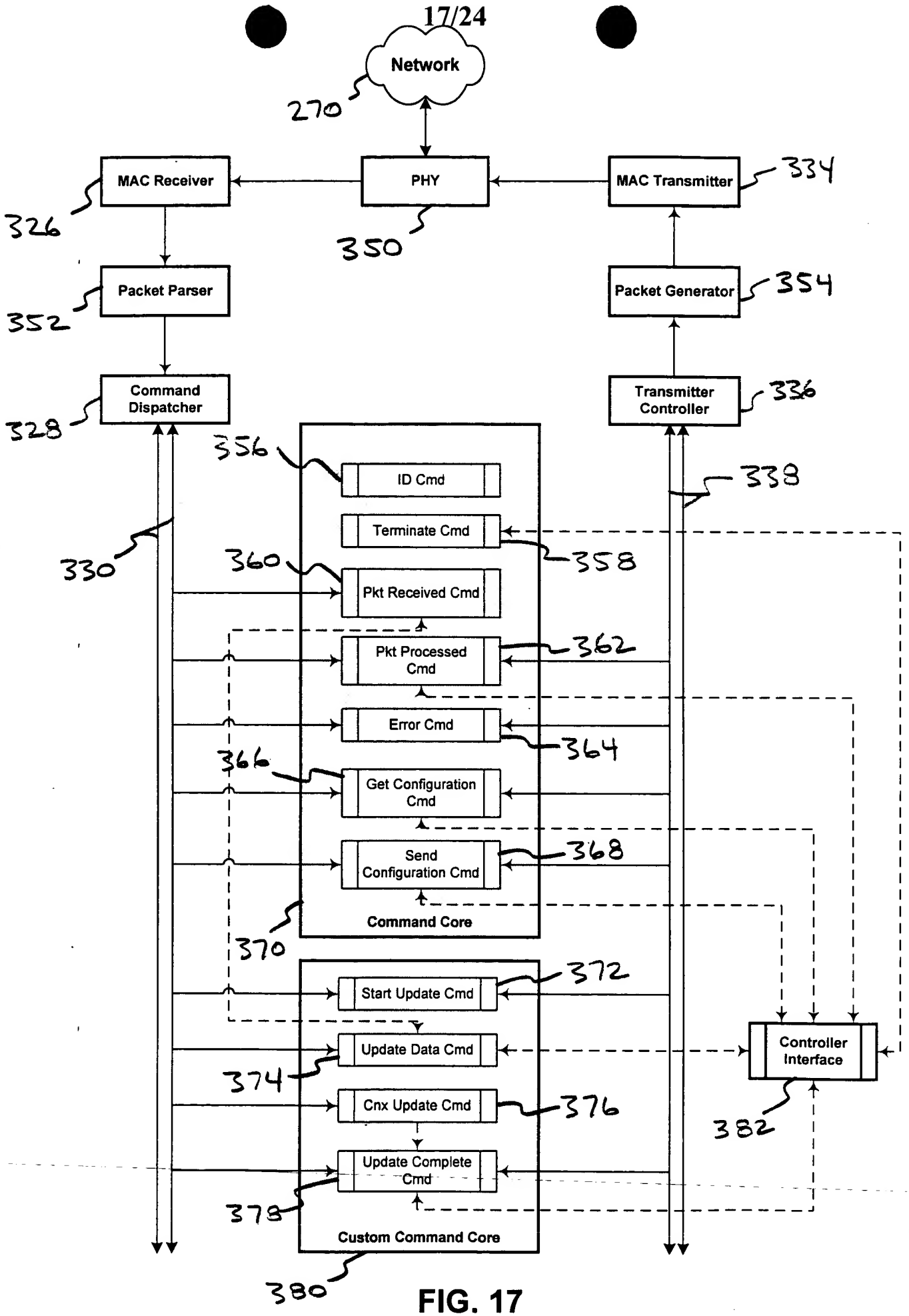
Network
270
MAC Receiver
326
PHY
350
MAC Transmitter
334
Packet Parser
352
Packet Generator
354
Command Dispatcher
328
Transmitter Controller
336
356
ID Cmd
338
Terminate Cmd
330
358
360
Pkt Received Cmd
Pkt Processed Cmd
362
Error Cmd
364
366
Get Configuration Cmd
Send Configuration Cmd
368
Command Core
370
372
Start Update Cmd
Update Data Cmd
Controller Interface
374
Cnx Update Cmd
376
382
Update Complete Cmd
378
Custom Command Core
380

FIG. 17

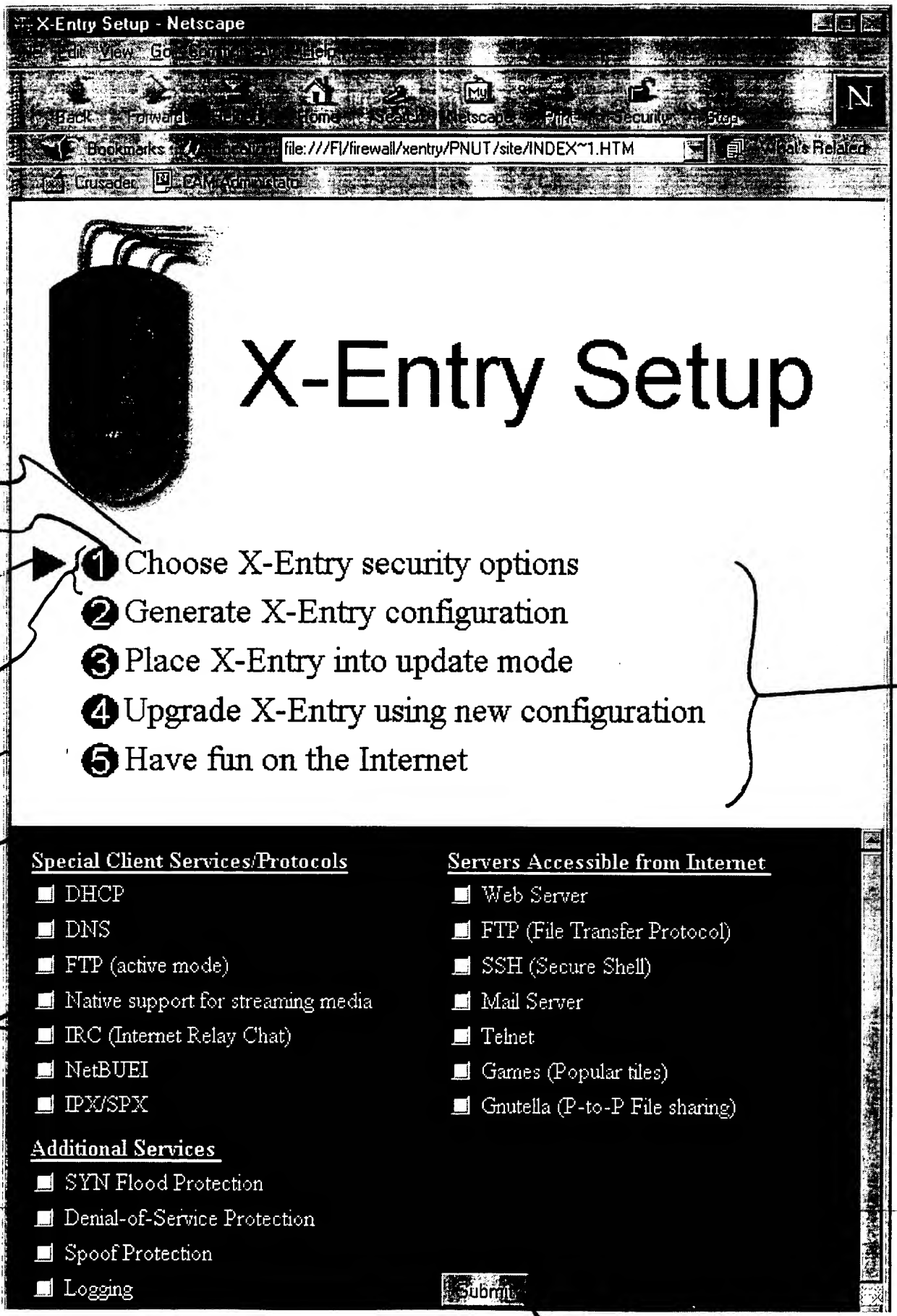
X-Entry Setup - Netscape
file:///F|/firewall/xentry/PNUT/site/INDEX~1.HTM
X-Entry Setup
1 Choose X-Entry security options
2 Generate X-Entry configuration
3 Place X-Entry into update mode
4 Upgrade X-Entry using new configuration
5 Have fun on the Internet
Special Client Services/Protocols
DHCP
DNS
FTP (active mode)
Native support for streaming media
IRC (Internet Relay Chat)
NetBUEI
IPX/SPX
Servers Accessible from Internet
Web Server
FTP (File Transfer Protocol)
SSH (Secure Shell)
Mail Server
Telnet
Games (Popular tiles)
Gnutella (P-to-P File sharing)
Additional Services
SYN Flood Protection
Denial-of-Service Protection
Spoof Protection
Logging
Submit
391
393
390
392
384
388
394
386
396

FIG. 18

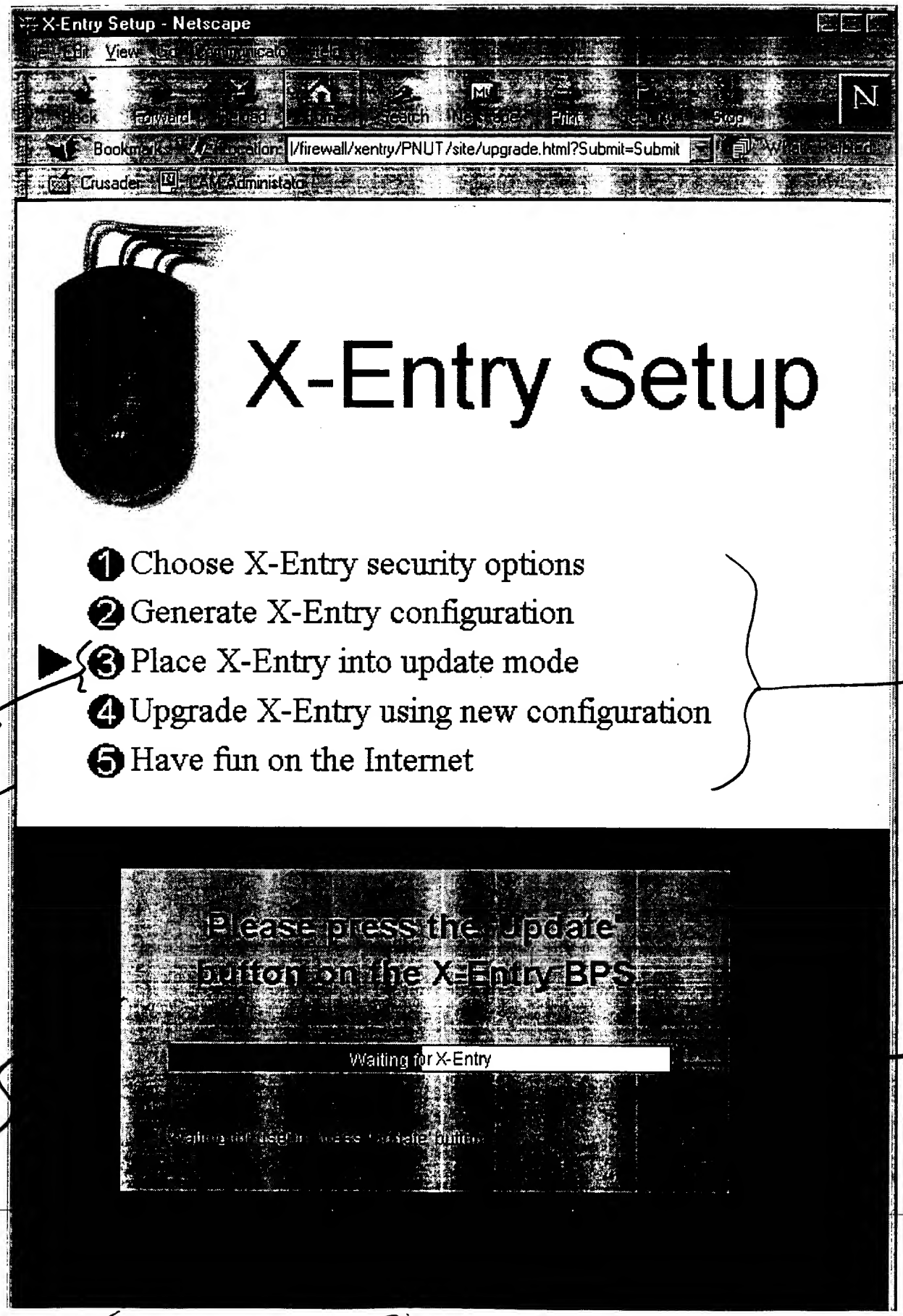
X-Entry Setup - Netscape
/firewall/xentry/PNUT/site/upgrade.html?Submit=Submit
X-Entry Setup
1 Choose X-Entry security options
2 Generate X-Entry configuration
3 Place X-Entry into update mode
4 Upgrade X-Entry using new configuration
5 Have fun on the Internet
Please press the 'Update' button on the X-Entry BPS
Waiting for X-Entry
398
384
386
400
402
404

FIG. 19

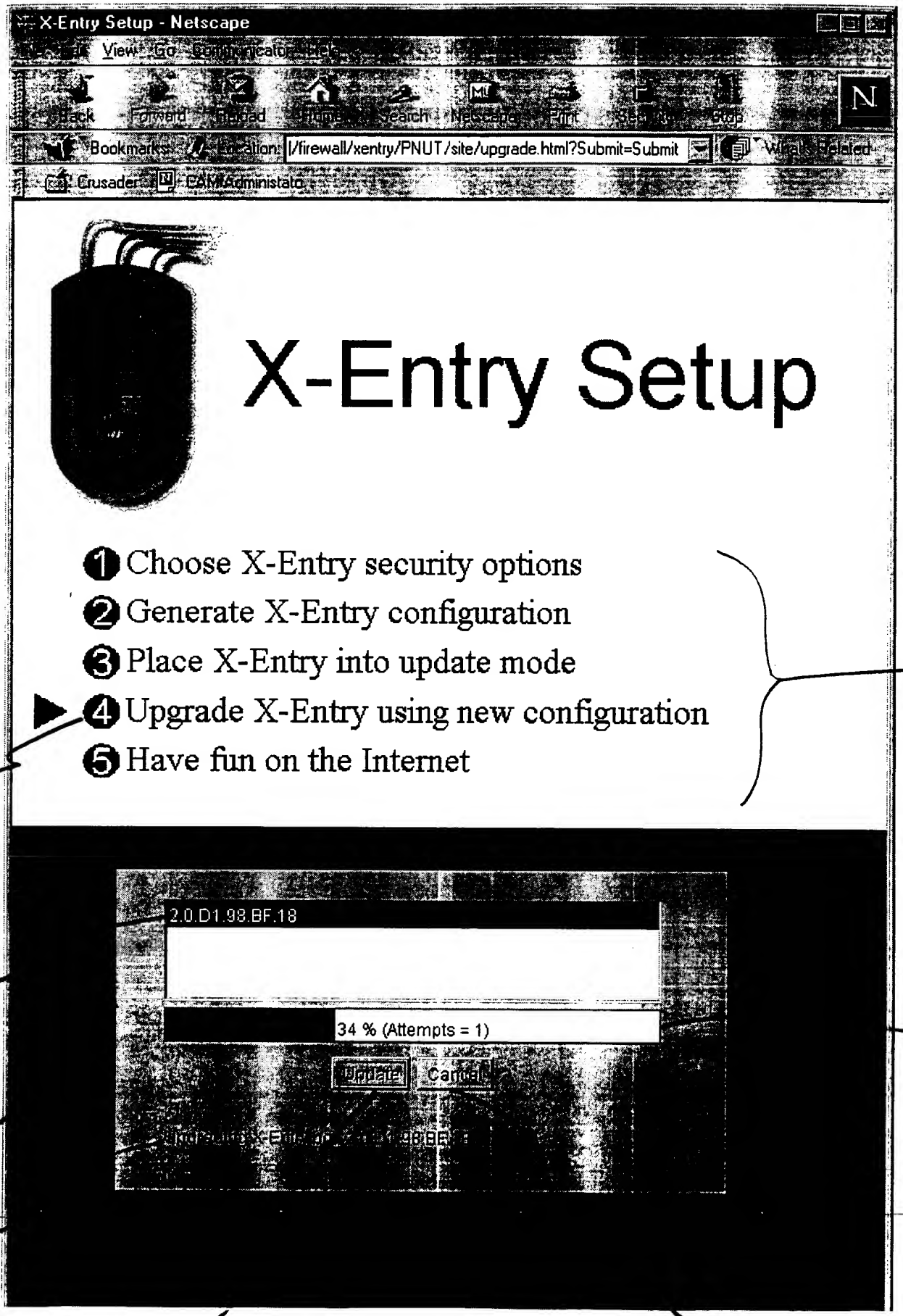
X-Entry Setup - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: /firewall/xentry/PNUT/site/upgrade.html?Submit=Submit
What's Related
Crusader CAM Administrator
X-Entry Setup
1 Choose X-Entry security options
2 Generate X-Entry configuration
3 Place X-Entry into update mode
4 Upgrade X-Entry using new configuration
5 Have fun on the Internet
336
406
2.0.D1.98.BF.18
34 % (Attempts = 1)
Update
Cancel
410
414
408
412
416
418

FIG. 20

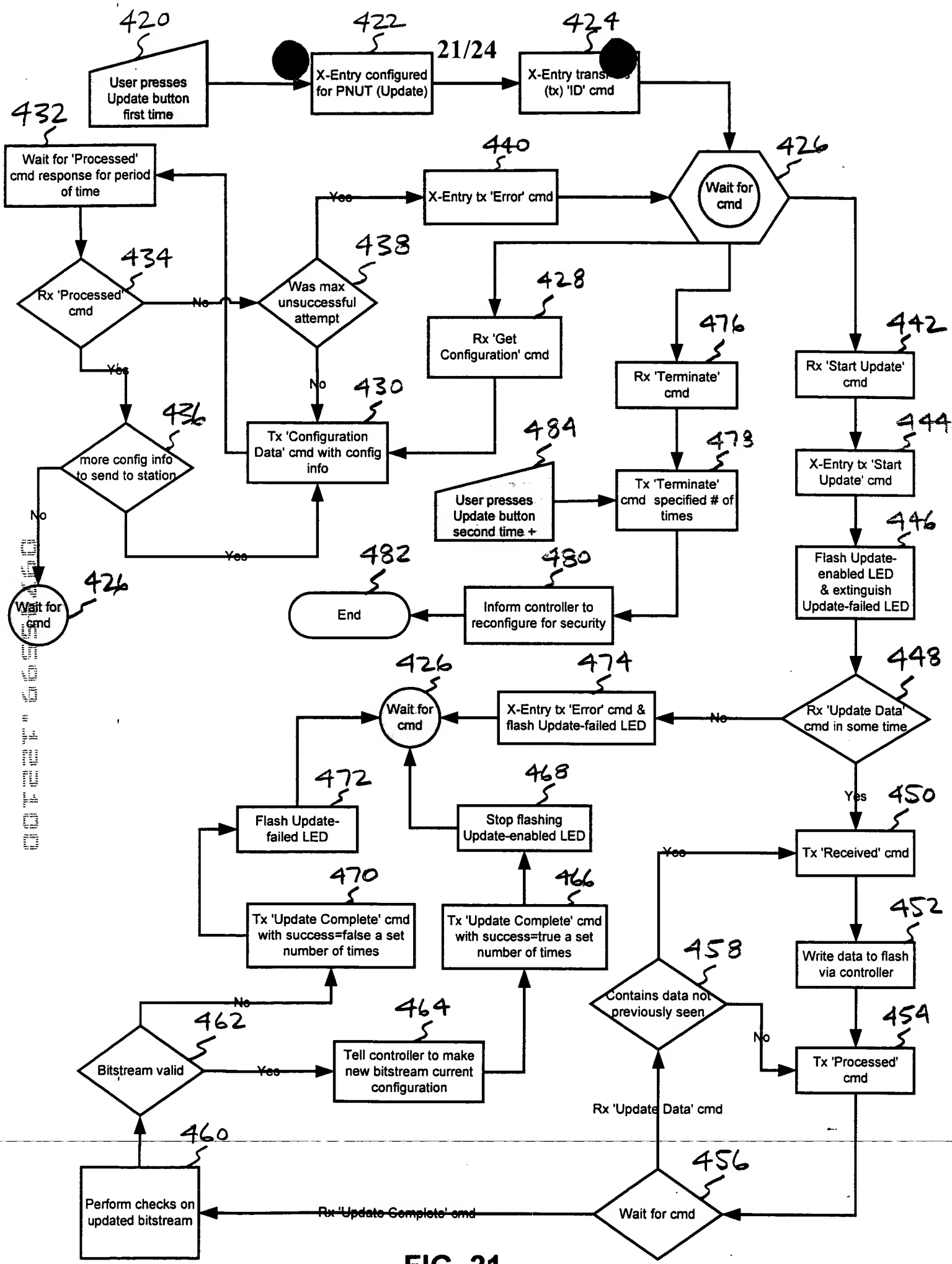
420
User presses Update button first time
422
X-Entry configured for PNUT (Update)
424
X-Entry transmits (tx) 'ID' cmd
426
Wait for cmd
432
Wait for 'Processed' cmd response for period of time
434
Rx 'Processed' cmd
Yes
No
436
more config info to send to station
No
Yes
438
Was max unsuccessful attempt
Yes
No
440
X-Entry tx 'Error' cmd
428
Rx 'Get Configuration' cmd
430
Tx 'Configuration Data' cmd with config info
476
Rx 'Terminate' cmd
478
Tx 'Terminate' cmd specified # of times
484
User presses Update button second time +
480
Inform controller to reconfigure for security
482
End
442
Rx 'Start Update' cmd
444
X-Entry tx 'Start Update' cmd
446
Flash Update-enabled LED & extinguish Update-failed LED
448
Rx 'Update Data' cmd in some time
No
474
X-Entry tx 'Error' cmd & flash Update-failed LED
Yes
450
Tx 'Received' cmd
452
Write data to flash via controller
454
Tx 'Processed' cmd
458
Contains data not previously seen
No
Yes
Rx 'Update Data' cmd
456
Wait for cmd
Rx 'Update Complete' cmd
460
Perform checks on updated bitstream
462
Bitstream valid
No
Yes
464
Tell controller to make new bitstream current configuration
466
Tx 'Update Complete' cmd with success=true a set number of times
468
Stop flashing Update-enabled LED
470
Tx 'Update Complete' cmd with success=false a set number of times
472
Flash Update-failed LED
426
Wait for cmd

FIG. 21

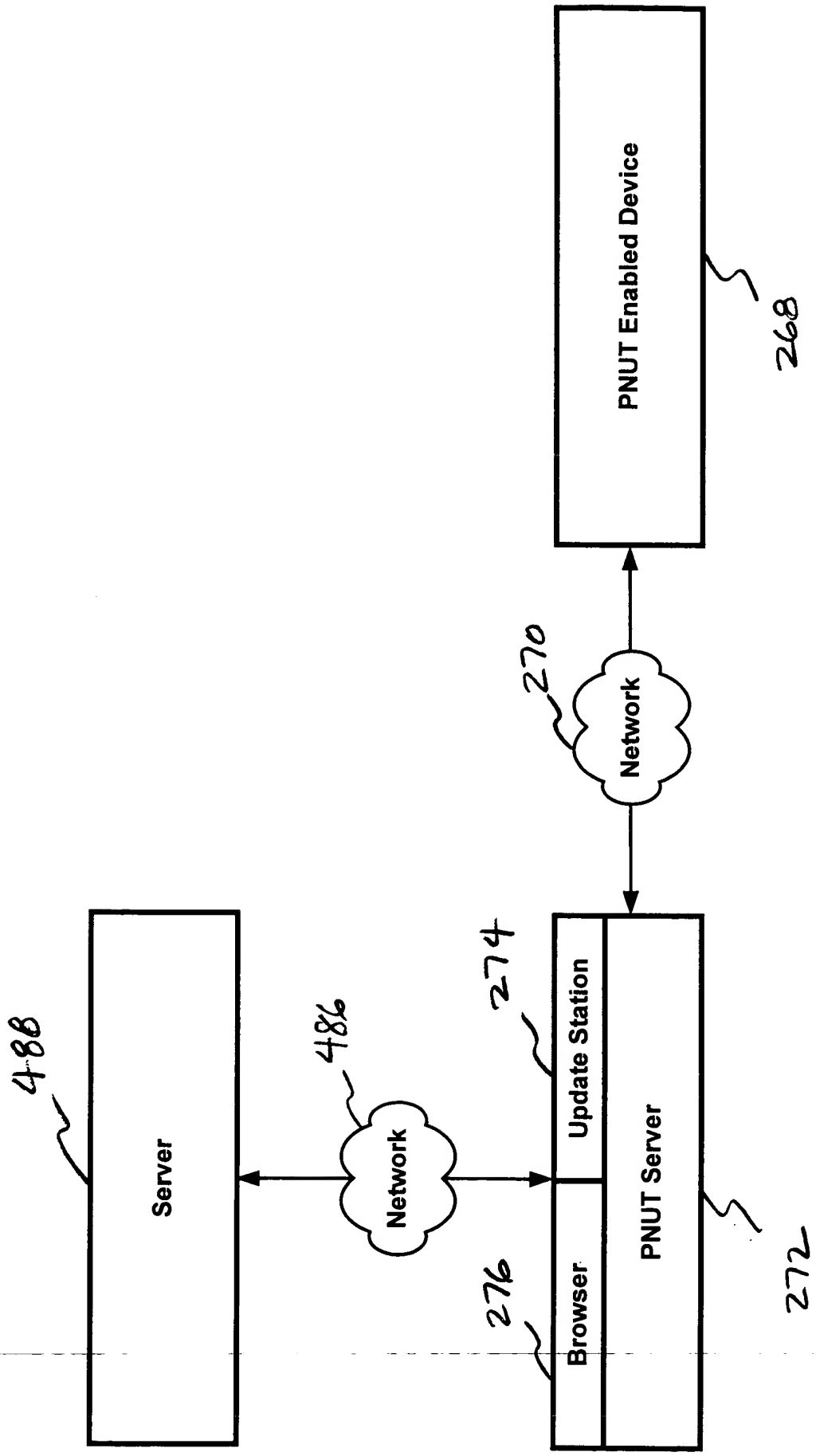
PNUT Enabled Device
268
Network
270
Update Station
274
PNUT Server
272
Browser
276
Network
486
Server
488

FIG. 22

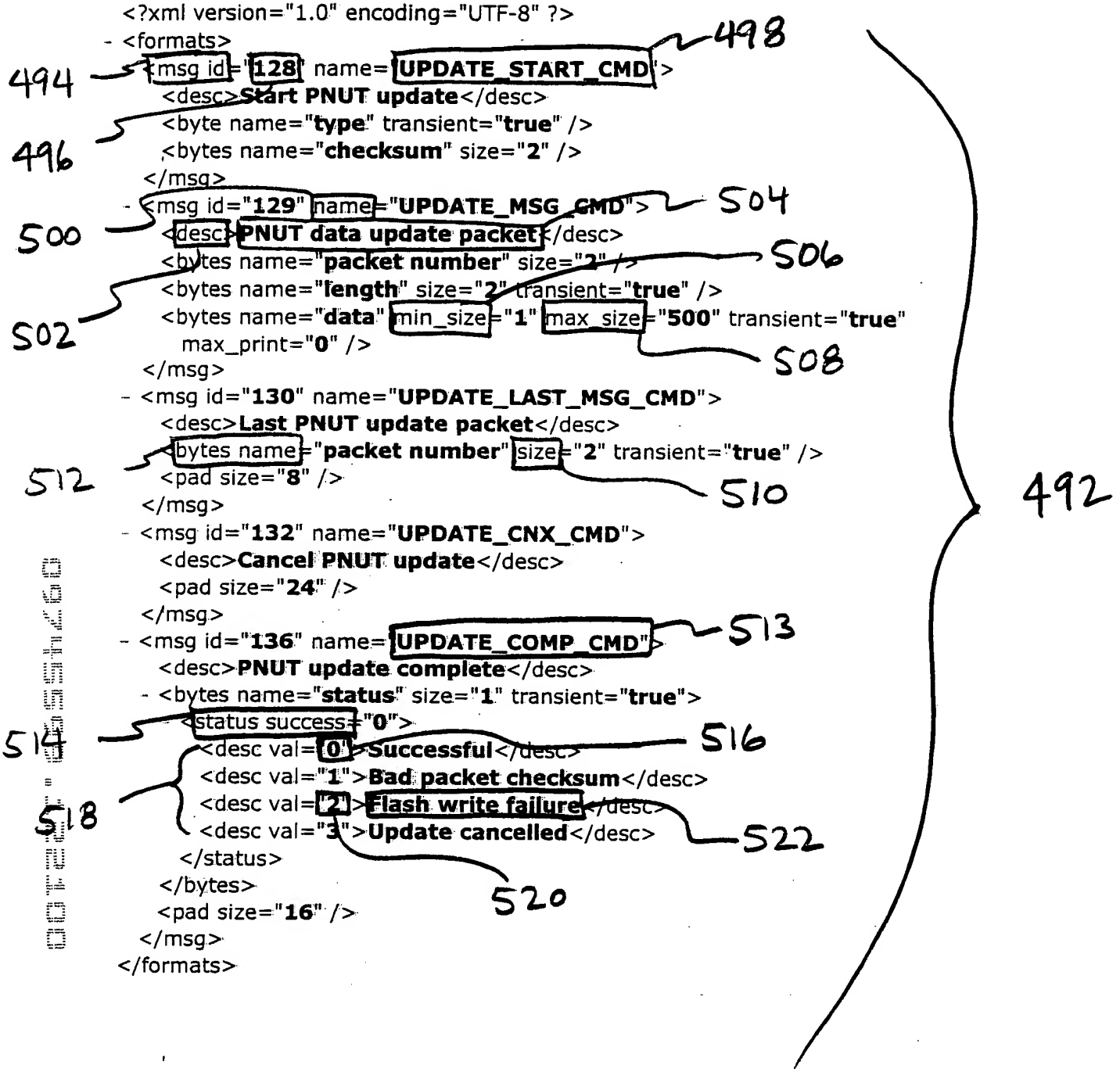
<?xml version="1.0" encoding="UTF-8" ?>
- <formats>
<msg id="128" name="UPDATE_START_CMD">
<desc>Start PNUT update</desc>
<byte name="type" transient="true" />
<bytes name="checksum" size="2" />
</msg>
- <msg id="129" name="UPDATE_MSG_CMD">
<desc>PNUT data update packet</desc>
<bytes name="packet number" size="2" />
<bytes name="length" size="2" transient="true" />
<bytes name="data" min_size="1" max_size="500" transient="true"
max_print="0" />
</msg>
- <msg id="130" name="UPDATE_LAST_MSG_CMD">
<desc>Last PNUT update packet</desc>
<bytes name="packet number" size="2" transient="true" />
<pad size="8" />
</msg>
- <msg id="132" name="UPDATE_CNX_CMD">
<desc>Cancel PNUT update</desc>
<pad size="24" />
</msg>
- <msg id="136" name="UPDATE_COMP_CMD">
<desc>PNUT update complete</desc>
- <bytes name="status" size="1" transient="true">
<status success="0">
<desc val="0">Successful</desc>
<desc val="1">Bad packet checksum</desc>
<desc val="2">Flash write failure</desc>
<desc val="3">Update cancelled</desc>
</status>
</bytes>
<pad size="16" />
</msg>
</formats>
494
496
498
500
502
504
506
508
510
512
513
514
516
518
520
522
492

FIG. 23

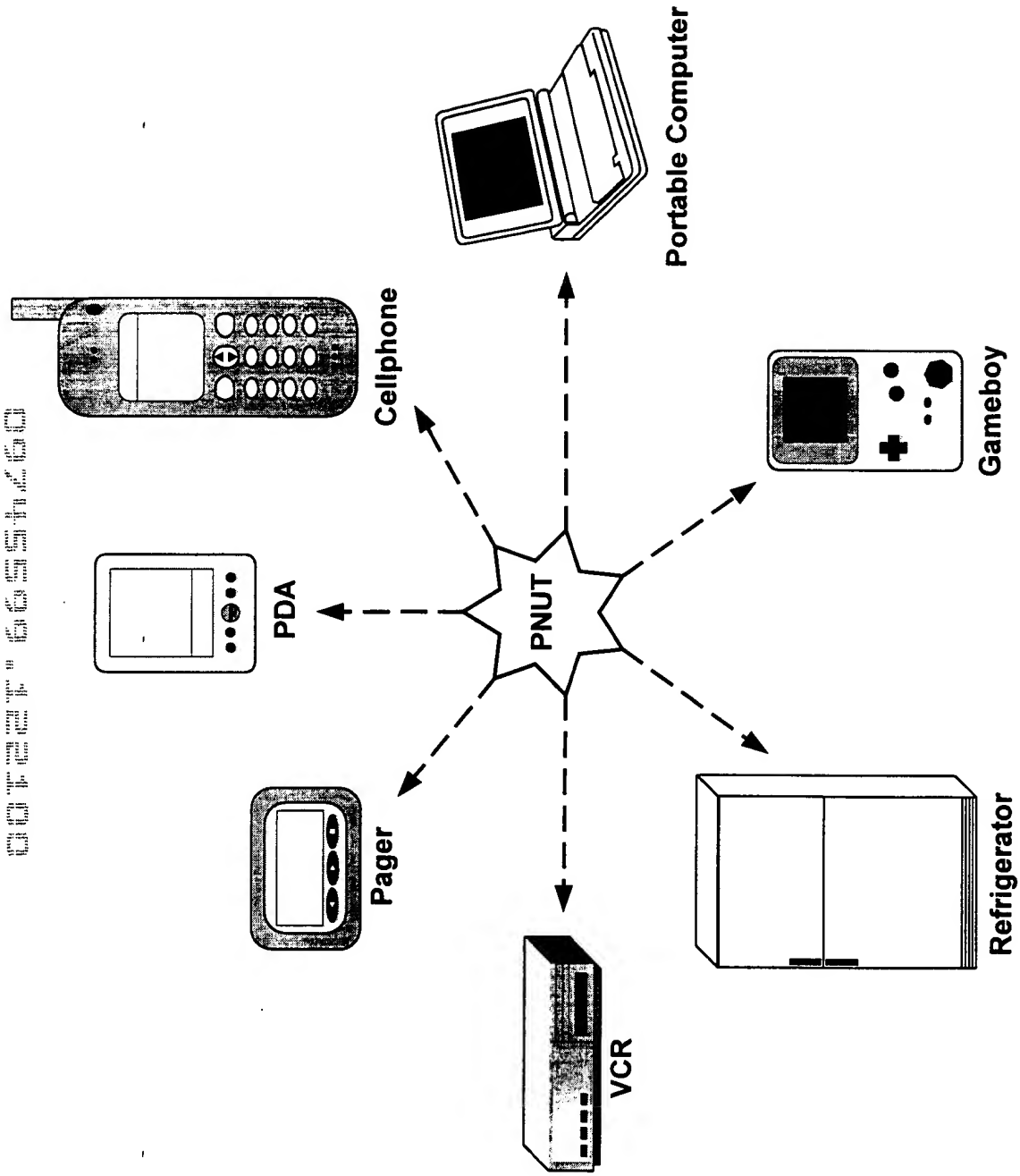
Portable Computer
Cellphone
Gameboy
PDA
PNUT
Pager
Refrigerator
VCR

FIG. 24